AMENDMENTS TO THE CLAIMS

1-46.(Cancelled)

47. (New) A method for analyzing or selectively modifying or filtering data packets passing through a device placed on an edge in a computer network, said device comprising a processor that runs a compiler and a piece of software in accordance with a security policy, said software being designed to filter said data packets, thereby authorizing or not authorizing their passage in accordance with said security policy, the method comprising the steps of:

defining said security policy by portable agents written in a computer language that is independent of the language of said processor and for analyzing, selectively modifying or selectively filtering said data packets;

automatically calling said compiler by said software in order to perform a compilation for translating said portable agents into executable agents written in the language of said processor;

running said software in order to filter said data packets passing through said device, thereby authorizing or not authorizing their passage in accordance with said security policy; and

performing at least one of the following steps:

analyzing said data packets authorized by said software to pass through said device, by executing said executable agents by said processor;

selectively modifying said data packets authorized by said software to pass through said device, by executing said executable agents by said processor; or

selectively filtering said data packets authorized by said software to pass through said device, by executing said executable agents by said processor.

48. (new) The method of claim 47, wherein said security policy comprises a definition of various objects of said computer network.

49. (new) The method of claim 47, wherein said security policy comprises a definition of various services of said computer network.

50. (new) The method of claim 47, wherein said security policy comprises a definition of various users of said computer network.

51. (new) The method of claim 50, further comprising the step of generating configuration parameters, thereby enabling the configuration of said portable agents based on said users of said computer network.

52. (new) The method of claim 47, wherein said security policy comprises a definition of said device.

53. (new) The method of claim 47, wherein said computer language is a low-level language that is dedicated to operations on said data packets of said computer network, thereby monitoring and limiting the possible actions of said portable agents inside said device.

54. (new) The method of claim 47, further comprising the step of defining said security policy in a server remote from said device.

55. (new) The method of claim 47, further comprising the step of defining said security policy in said device.

56. (new) The method of claim 47, further comprising the step of authenticating the non-authenticated user of said device to provide an authenticated user of said device.

57. (new) The method of claim 56, wherein said security policy comprises a definition of said authenticated user of said device.

58. (new) The method of claim 57, wherein the step of authenticating uses an identification means associated with said device to authenticate said non-authenticated user of said device.

59. (new) The method of claim 57, wherein the step of authenticating uses a server application of a client/server application in said device to authenticate said non-authenticated user of said device.

60. (new) The method of claim 47, further comprising the step of executing functions from a function library of said software and called by said executable agents.

61. (new) The method of claim 60, further comprising the step of executing specialized functions from said function library for managing a cache of said data packets.

62. (new) The method of claim 61, wherein the step of executing specialized functions further comprises the steps of:

storing in said cache, after the execution of said executable agents, packet information concerning said data packets and said data packets if said data packets have been modified during the execution of said executable agents;

verifying whether an incoming packet in said device is a packet that has already been received by said device based on said packet information stored in said cache;

executing said executable agents if it is determined that said incoming packet is not a packet that has already been received by said device;

determining whether said incoming packet has been modified by said executable agents using said packet information stored in said cache if it is determined that said incoming packet is a packet that has already been received;

transmitting a version of said incoming packet stored in said cache to said computer network without executing said executable agents if it is determined that said already received packet has been modified by said executable agents; and

transmitting said incoming packet to said computer network without executing said executable agents if it is determined that said incoming packet has not been modified by said executable agents.

63. (new) The method of claim 60, further comprising the step of executing specialized functions from said function library for managing said computer network and transport layers of the communication protocol used.

64. (new) The method of claim 63, wherein the step of executing specialized functions comprises the steps of:

storing protocol information from said computer network and said transport layers of said data packets passing through said device to monitor various flows of said data packets;

storing any modifications of said data packets performed by said executable agents;

updating said protocol information from said computer network and said transport layers of said data packets passing through said device, based on said protocol information and said stored modifications, in said data packets so as to maintain consistency in the flows of said data packets .

65. (new) The method of claim 60, further comprising the step of executing specialized functions from said function library for searching for regular patterns and expressions.

66. (new) The method of claim 60, further comprising the step of executing specialized functions from said function library for communicating between said executable agents.

67. (new) The method of claim 60, further comprising the step of executing specialized functions from said function library for communicating between said executable agents and objects of said computer network.

68. (new) The method of claim 60, further comprising the step of associating specialized hardware components of said device with functions of said function library to accelerate the execution of said functions.

69. (new) The method of claim 47, further comprising the step of modifying said security policy by executing said executable agents by said processor.

70. (new) A system for analyzing or selectively modifying or filtering data packets, comprising:

a device placed on an edge in a computer network, said device comprising a processor that runs a compiler and a piece of software in accordance with a security policy, said software comprising a filter for filtering said data packets passing through said device, thereby authorizing or not authorizing the passage of said packets in accordance with said security policy, and

portable agents for defining said security policy written in a computer language that is independent of the language of said processor and for analyzing or selectively modifying or filtering said data packets; and

wherein said software is operable to automatically activate said compiler to translate said portable agents into executable agents written in the language of said processor; and

wherein said process is operable to execute said executable agent to perform at least one of the following:

analyze said data packets authorized by said software to pass through said device;

selectively modify said data packets authorized by said software to pass through said device; or

selectively filter said data packets authorized by said software to pass through said device.

71. (new) The system of claim 70, wherein said security policy comprises a definition of various objects of said computer network.

72. (new) The system of claim 70, wherein said security policy comprises a definition of various services of said computer network.

73. (new) The system of claim 70, wherein said security policy comprises a definition of various users of said computer network.

74. (new) The system of claim 73, further comprising a module for generating configuration parameter for configuring said portable agents based on said users of said computer network.

75. (new) The system of claim 70, wherein said security policy comprises a definition of said device.

76. (new) The system of claim 70, wherein said computer language is a low-level language that is dedicated to operations on said data packets of said computer network thereby monitoring and limiting the possible actions of said portable agents in said device.

77. (new) The system of claim 70, further comprising a server, remote from said device, for defining said security policy.

78. (new) The system of claim 70, wherein said device comprises an administrative module for defining said security policy.

79. (new) The system of claim 70, further comprising an authentication device for authenticating non-authenticated user or users of said device to provide an authentication user of said device.

80. (new) The system of claim 79, wherein said security policy comprises a definition of said authenticated users of said device.

81. (new) The system of claim 80, wherein said device comprises an identification device for authenticating said non-authenticated user of said device.

82. (new) The system of claim 80, wherein said device comprises a server application of a client/server application operable to authenticate said non-authenticated user of said device.

83. (new) The system of claim 70, wherein said software comprises a function library comprising functions callable by said executable agents.

84. (new) The system of claim 83, wherein said function library comprises specialized functions for managing a cache of said data packets.

85. (new) The system of claim 84, wherein said cache of said data packets comprises:

a memory for storing, after the execution of said executable agents, packet information concerning said data packets, and said data packets;

a verification module for verifying, based on said packet information stored in said cache, whether an incoming packet is a packet that has already been received and whether said incoming packet has been modified by said executable agents; and

an activation module for activating a transmitter for transmitting said incoming data packet stored in said memory to said computer network without modification if it is determined that said incoming packet has been modified by said verification module or a transmitter or for transmitting said incoming packet to said computer network without modification if it is determined that said incoming packet has not been modified by said verification means.

86. (new) The system of claim 83, wherein said function library comprises specialized functions for managing the network and transport layers of the communication protocol used.

87. (new) The system of claim 86, wherein said device comprises:

at least one memory for storing protocol information from said computer network and said transport layers of said data packets passing through said device for monitoring various flows of said data packets and storing any modifications of said data packets performed by said executable agents; and

a module for updating said protocol information from said computer network and said transport layers of said data packets passing through said device, based on said protocol information and said stored modifications, in said data packets so as to maintain consistency in the flows of said data packets.

88. (new) The system of claim 83, wherein said function library comprises specialized functions for searching for regular patterns and expressions.

89. (new) The system of claim 83, wherein said function library comprises specialized functions for communicating between said executable agents.

90. (new) The system of claim 83, wherein said function library comprises specialized functions for communicating between said executable agents and objects of said computer network.

91. (new) The system of claim 83, wherein said device comprises specialized hardware components associated with functions of said function library to accelerate the execution of said functions.

92. (new) The system of claim 70, wherein said executable agents executed by said processor is operable to modify said security policy.